IPTABLES: Aprenda Como Utilizar A Principal Ferramenta Para Implementar Firewall No Linux

pedrodelfino

JUNTE-SE A MAIS DE 110.000 PESSOAS QUE JÁ TEM UMA CÓPIA

Ubuntu: Iniciando Com Linux De Maneira Prática E Rápida

Compartilhe Este Post

Se você vem acompanhando a série de artigos nos quais abordo as principais soluções de firewall para Linux, certamente já esperava por uma publicação especial sobre a ferramenta mais influente da categoria: o iptables.

Por que me sinto tão seguro em afirmar que o iptables é influente a tal ponto? Simplesmente, este firewall é amplamente utilizado entre especialistas em Segurança da Informação, tanto pelos recursos oferecidos, quanto pelo fato de ser um programa compatível com qualquer distribuição.

Não podemos ignorar, também, a influência do iptables para o surgimento de novas soluções de alto nível, como o nftables — confira este artigo sobre nftables e compreenda a relação. Logo, estou falando de uma aplicação relevante no contexto histórico e, ao mesmo tempo, um grande legado.

Sabendo da importância do iptables quando o assunto é firewall Linux, que tal conhecê-lo mais a fundo (inclusive as suas funcionalidades), aprender a instalá-lo e configurá-lo em seu ambiente de trabalho? Só continuar a leitura!

Definição do iptables

O iptables não é essencialmente um firewall, mas um programa que, por meio de seus módulos, possibilita ao usuário configurar o kernel Linux e o conjunto de regras do filtro de pacotes — função típica do firewall.

Na prática, o administrador de sistemas tem de gerenciar quatro tabelas (filter, NAT, mangle e security) com funções distintas e, com isso, aplicar as regras desejadas. Como a interação ocorre quase diretamente com o kernel, praticamente não há limites quanto à aplicação de regras via iptables.

Instalação do iptables no CentOS

Embora as versões atuais do CentOS utilizem o Firewalld como solução padrão, cabe explicar que mantê-lo instalado é uma opção. Logo, se você deseja testar o iptables numa distribuição voltada a ambientes corporativos, como é o caso do CentOS, siga as instruções:

```
sudo yum install iptables-services

sudo systemctl start iptables

sudo systemctl start iptables6

sudo systemctl enable iptables # o comando enable ativará a inicializa

sudo systemctl enable iptables6
```

```
sudo systemctl status iptables # este comando nos retornará o status d

sudo systemctl status iptables6
```

Concluídas as breves etapas acima o iptables estará pronto para entrar em ação.

Cinco configurações e comandos básicos do firewall

Um detalhe que deve ficar bem esclarecido: o iptables, como o próprio nome diz, trabalha com um sistema de tabelas. Portanto, aconselho que leia este artigo no qual explico as tabelas do iptables antes de aprofundar-se nos estudos. Abaixo, cinco comandos que você pode testar em seu firewall Linux.

Verificar todas as regras existentes

Uma ação bastante útil para começar a praticar o iptables é solicitar uma lista que contenha todas as regras que já estão

em vigor. Faça isso digitando o comando **iptables -L -n -v** — repare que o iptables retornará uma lista geral.

Também é possível consultar as regras de uma tabela em especial. Por exemplo, se quisermos analisar a tabela filter, basta digitarmos **iptables -t filter -L -v -n**. Muito simples, não é mesmo?

Bloquear sites indesejados via iptables

Do ponto e vista de gestores e líderes de negócios, uma das maiores utilidades de um firewall na rede corporativa é garantir que os funcionários não se ocupem navegando em sites que estimulem a improdutividade, tais como as redes sociais.

No iptables, bloquear o acesso a determinados conteúdos é muito simples. Supondo que o conteúdo em questão seja o Facebook, tudo que precisamos fazer é descobrir o IP do site e, em seguida, aplicar a regra. Primeiramente, vamos acionar o comando host:

```
#host facebook.com

Output:

facebook.com has address 157.240.12.35

facebook.com has IPv6 address 2a03:2880:f105:283:face:b00c:0:25de

facebook.com mail is handled by 10 smtpin.vvv.facebook.com.
```

Copie o IP (157.240.12.35) e digite no iptables a seguinte linha:

```
# iptables -A OUTPUT -p tcp -d 157.240.12.35 -j DROP
```

Proceda da mesma maneira para bloquear os sites que compõem a lista negra do seu chefe ou da sua própria empresa.

Impedir o servidor de receber ping

Tendo em vista aprimorar a segurança do servidor Linux, o administrador de sistemas tem a opção de bloquear requisições de ping. Em outras palavras, impedir que qualquer outro computador utilize o comando ping para obter informações sobre o servidor.

No iptables, o comando para aplicar a regra é esse:

```
# iptables -A INPUT -p icmp -i eth0 -j DROP
```

Vale frisar que eth0 corresponde à interface de rede do servidor. Para descobrir as interfaces disponíveis em sua rede, utilize um dos comandos abaixo:

```
$ netstat -i

# requer instalação (yum -y install net-tools)

$nmcli device status
```

```
$ ip link show
```

Delimitar conexões simultâneas por IP

Outro recurso interessante do iptables para controlar a rede é a delimitação de conexões por IP. Além de impor regras dentro do ambiente de trabalho, o comando que veremos abaixo é ótimo para reduzir o consumo de banda larga.

Supondo que cada usuário tenha o direito a até quatro conexões, digite:

```
# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-al
```

Em destaque: o comando connlimit, usado especialmente para estabelecer limites de conexão, e o número 4 como indicador.

Bloquear um IP específico

Ao monitorar a rede de computadores, o administrador de sistemas pode identificar atividades suspeitas ou abusivas, as quais devem ser coibidas imediatamente. O processo para isso é muito simples, bastando ao sysadmin pegar o endereço de IP do alvo e inseri-lo no seguinte comando:

```
# iptables -A INPUT -s 000.000.000.000 -j DROP
```

Mas como realizar o desbloqueio do respectivo IP? Acione a

opção -D (ou –delete) para remover a regra em questão.

```
# iptables -D INPUT -s 000.000.000.000 -j DROP
```

A flag -D, inclusive, se aplica a qualquer regra que o usuário queira eliminar.

Gostou das regras elencadas até aqui? Se sim, fique atento aos próximos conteúdos sobre firewall ou, se preferir, deixe um comentário pedindo uma publicação especial de comandos do iptables, fechado?

Convém destacar, no entanto, que o site Profissionais Linux o possibilita a descobrir um meio rápido e eficaz para especializar-se em tudo que envolve o sistema Linux, inclusive as soluções de firewall. Confira!

Artigos Relacionados:

Grub: Tudo Sobre O Gerenciador de Boot Do Linux

LAMP no Linux: Aprenda a Instalar e Crie um Servidor WEB em Seu VPS

MongoDB - Guia básico para instalar um banco de dados NoSQL no Linux

Lynx: Como Navegar Pela WEB Usando o Modo Texto No Linux (+5 Alternativas)

Compartilhe Este Post

ANTERIOR
NFtables: Aprenda Como Utiliz...

PRÓXIMO
Servidor De Arquivos: Como I...

Artigos Recentes

Linux

Zabbix: O Que É, Para Que Serve E Como Instalar Nas Distros Debian E CentOS

Após cerca de 20 anos desde o lançamento da primeira versão beta, muitas empresas no mundo inteiro optam por instalar Zabbix a fim agregar inteligência

pedrodelfino

Linux

Linux

O Que É Kubernetes E Como A Tecnologia É Utilizada Pelas Empresas?

Kubernetes (kube ou K8) é uma plataforma open source projetada para automatização e orquestração de operações de contêineres Linux, como o Docker. Como toda automação, a

pedrodelfino

Descubra Nossos E-books

Conteúdos extras e aprofundados para você ler onde estiver

"*Um dos projetos que criei já ajudou mais de 110 mil pessoas a aprender LINUX ...*"

Pedro Delfino
FUNDADOR DO PROFISSIONAIS LINUX

Sobre Pedro Delfino

FUNDADOR DO PROFISSIONAIS LINUX

Eu sou Pedro Delfino que durante os últimos 18 anos estive envolvido em implantações de soluções de TI utilizando LINUX, enquanto estava á frente de uma equipe de TI.

Fundador do Profissionais Linux que hoje já conta com mais de 2100 alunos, fui o responsável por diversos projetos de sucesso, todos eu sempre foquei o resultado em primeiro lugar, ou seja, sempre quando crio uma nova solução com Linux que será implantada estou procurando um objetivo especifico.

QUERO ACESSAR AGORA

Você deseja aprender e dominar o Linux de uma vez por todas?

MÉTODO Ensina como Sair do ZERO em LINUX se Tornar um PROFISSIONAL QUALIFICADO em administração de servidores.

Cursos
Materiais
Blog
Contato